INCIDENT HANDLING POLICY, PROCEDURES, AND TOOLS

As more organizations connect to the Internet and share information globally, the need for a rapid incident handling capability increases. The number of Internet related incidents that have occurred in the past year require organizations to take seriously their incident handling capability. The Office of Management and Budget has reinforced this need by requiring in the newly revised OMB Circular A-130, that federal agencies be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. This new requirement comes at a time when federal agencies are being faced with reduced budgets and staff. Many organizations have already developed incident handling teams or incident handling procedures. This panel will discuss the incident handling policy and procedures that have been implemented within their organizations. In addition, a new methodology that system administrators can use for characterizing network security tools will be discussed.

Chair:
Marianne Swanson, National Institute of Standards and Technology

Panelists:
Kelly Cooper, BBN Planet
BBN Planet is an Internet Service Provider. As a service provider they notify their customers of major security events and problems and field calls from customers asking for information on and help with incidents. When an incident is reported, BBN's goals are (a) to perform identification of the problem (to confirm whether the situation is a security incident and determine the seriousness of the problem), (b) to do damage control (i.e. making router filters more restrictive or taking the customer off the net until they have repaired their breach), and © to provide encouragement to the customer in contacting other sites involved. They also provide basic information on policies/procedures and direct customers to CERT's patches, tools and information. The practices and procedures that BBN uses in their incident handling efforts will be presented.

Thomas Longstaff, Computer Emergency Response Team/Coordination Center (CERT/CC)
This presentation will report on a new methodology for characterizing the capabilities of network security tools. This method determines what threats or risks are addressed by the collections of tools in a network environment. In particular, for each tool identified, it is possible to determine what the tools do and what threats or risks are addressed. From this assessment, a network administrator will be able to determine which risks are managed appropriately and use the result as a guide for acquiring new network security tools. In addition, it will be possible to use the method to determine if existing tools cover newly discovered vulnerabilities or if a newly developed tool will cover additional threats. Unlike an evaluation of a security tool, this method does not address the "goodness" of the security tool, but only its designed capabilities. As a practical example, we will provide the results of applying the methodology to a representative set of existing tools to identify what threats they cover in a network environment.

Peter Richards, Westinghouse Savannah River Company
The Department of Energy's CIAC response team is used to augment Savannah River's incident handling capability. Many organizations are employing outside assistance to handle incidents if they become too large in scope or too difficult to handle in house. This type of incident handling support is being implemented more frequently. The policy and procedures that are used in this company will be discussed.

Ken van Wyk, Science Applications International Corporation (SAIC)
SAIC's Security Emergency Response Center (SERC) provides fee-for-service assistance to commercial and government organizations in need of on-call and on-site security incident response support. The procedures that SERC uses to handle their client's incidents will be reviewed.

Marianne Swanson, National Institute of Standards and Technology
National policy now requires agencies to develop an incident handling capability. NIST has been tasked to facilitate incident handling for the federal agencies by providing standards, guidance, and mechanisms for sharing information. The status of NIST's progress in this area will be presented.